RECEIVED
CENTRAL FAX CENTER
APR 07 2006

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application.

LISTING OF CLAIMS:

Claims 1 - 14 (Canceled).

15. (Previously Amended) A secure content object for distributing and controlling access to a document and annotations associated with the document, comprising:

an electronic document, the electronic document having been encrypted with a document encryption key, wherein access to the electronic document is available to a first set of authorized users;

an encrypted header comprising information pertaining to the electronic document;

a first multi-key encryption table for use in a multi-key encryption method associated with the electronic document, the first table comprising at least one multi-key component associated with each authorized user in the first set and a plurality of dummy encryption components, wherein the multi-key encryption table includes no information that may identify a user or the electronic document;

a plurality of annotations associated with the electronic document, generated by an annotation author and having been encrypted with an annotation encryption key, wherein access to the plurality of annotations is available to authorized annotation users comprising the annotation author and those users in the first set having been designated by the annotation author as having access to the plurality of annotations;

a second multi-key encryption table for use in a multi-key encryption method associated with the plurality of annotations, the second table comprising at least one multi-key component associated with each authorized annotation user; and

a user interface device comprising unencrypted information for identifying the electronic document and an interactive element for enabling a user to input a user authorization for access

to at least a portion of the encrypted electronic document, for inputting the user authorization to a decryption engine using the multi-key encryption method for combining the user authorization with each of the multi-key components in the first multi-key encryption key table to decrypt the encrypted header, and for combining the user authorization with each of the stored multi-key components in the second multi-key encryption key table to decrypt an annotation,

wherein upon a valid decryption of the annotation indicates the correct annotation encryption key has been found and the user is an authorized annotation user; and upon a valid decryption of the encrypted header, for enabling decryption of the portion of the encrypted electronic document.

16. (Original) The secure content object of claim 15, wherein the encrypted header includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the document encryption key has been found.

17. (Original) The secure content object of claim 15, wherein the electronic document comprises content information that is formatted based on an object language having a set of formatting rules.

18. (Original) The secure content object of claim 15, wherein the user interface device comprises a second electronic document.

19. (Original) The secure content object of claim 15, wherein the information pertaining to the electronic document comprises a user permission table for access to all or portions of the electronic document and wherein only those permitted portions of the electronic document are decrypted.

20. (Original) The secure content object of claim 15, wherein the encrypted header and the encrypted electronic document are encrypted using different encryption keys and

wherein the multi-key encryption table includes at least one multi-key component for each encryption key.

21. (Original) The secure content object of claim 15, wherein the encrypted header further comprises a fingerprint for identifying a predefined aspect of the electronic document.

22. (Original) The secure content object of claim 15, wherein the electronic document comprises a plurality of individual electronic documents, the encrypted header comprises information pertaining to each of the individual electronic documents.

23. (Original) The secure content object of claim 22, wherein the information pertaining to the electronic document comprises a user permission table setting forth access to all or portions of each of the individual electronic documents and wherein only those permitted portions of the authorized electronic document are decrypted.

24. (Original) The secure content object of claim 17, wherein the content information is selected from the group consisting of text, graphics, equations, tables, spreadsheets, pictures, video files, audio files, multimedia files and binary data of unknown format.

25. (Previously Presented) The secure content object of claim 17, wherein the object language comprises Adobe Acrobat.

26. (Previously Presented) The secure content object of claim 17, wherein the object language comprises a language which interprets Microsoft Word documents.

27. (Original) The secure content object of claim 20, wherein the encrypted header includes an encryption marker comprising a random number sequence followed by a

derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the header encryption key has been found; and wherein the encrypted electronic document includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the document encryption key has been found.

28. (Original) The secure content object of claim 15, wherein the electronic document includes a document ID and wherein the document encryption key includes a combination of the document ID, the user information and the multi-key component, for each authorized user.

29. (Original) The secure content object of claim 15, wherein the electronic document comprises a first electronic document and an annotation associated therewith, wherein the annotation is encrypted using an encryption key associated with a user generating the annotation; and wherein the encrypted header includes information pertaining to the first electronic document and the annotation.

30 - 34. (Canceled).

35. (Previously Amended) A method for creating a secure content object for distributing and controlling access to a document and annotations associated with the document, comprising:

providing an electronic document, wherein access to the electronic document is available to a first set of users;

responsive to a first user from the first set of users, generating a plurality of annotations pertaining to the electronic document using the document language and associating the plurality of annotations with the first user;

designating which users in the first set of users are authorized users have access to the

plurality of annotations;

encrypting each annotation using an annotation encryption key associated with the first user generating the particular annotation, wherein access to an encrypted annotation is available to authorized users having access to the respective annotation encryption key;

for each annotation encryption key:

generating a multi-key encryption table for use in a multi-key encryption method, the table comprising at least one multi-key component associated with each authorized user having been designated by the first user as having access to the annotation;

providing a user interface for enabling a user to input a user authorization for access to at least a portion of an encrypted annotation;

wherein, responsive to an input user authorization, combining the input user authorization with each of the stored multi-key components in the multi-key encryption key table to decrypt the annotation, wherein valid decryption of the annotation indicates the correct annotation encryption key has been found;

concatenating the plurality of encrypted annotations in a second electronic document; and

merging the second electronic document and the encrypted electronic document into a third electronic document such that access to the encrypted electronic document is available to the first set of users and access to the encrypted annotations in the separate file is provided only to authorized users.

36. (Canceled).

37. (Previously Presented) The method of claim 35, further comprising the step of encrypting the first electronic document using a document encryption key, wherein access to the encrypted electronic document is provided only to the first set of users;

generating a multi-key encryption table for use in a multi-key encryption method, the table comprising at least one multi-key component associated with each of the first set of users;

generating an encrypted header comprising information pertaining to the electronic

document;

providing a user interface for enabling a user to input a user authorization for access to at least a portion of the encrypted document;

combining the user authorization with each of the stored multi-key components in the multi-key encryption key table to decrypt the encrypted header; wherein valid decryption of the encrypted header indicates the document encryption key has been found.

38. (Original) The method of claim 35, further comprising adding an unencrypted header identifying the generating user to each encrypted annotation.

39. (Canceled).

40. (Canceled).

41. (Previously Presented) The method of claim 35, wherein the encrypted header includes an encryption marker comprising a random number sequence followed by a derivable variation of the same random number sequence, wherein a valid decryption of the encryption marker indicates the annotation encryption key has been found.

42. (Original) The method of claim 35, wherein the separate file and the electronic document are stored in different locations.